Nombres premiers

Définition

- Un entier naturel $p \geq 2$ est dit *premier*, si ses seuls diviseurs sont **1 et lui-même**.
- Un entier naturel, distinct de 1, non premier est appelé **entier composé**.

Exemple

1) Les six premiers nombres premiers sont : 2;3;5;7;11;13.

2) 6 et 121 ne sont pas des nombres premiers car : $6 = 2 \times 3$ et $121 = 11 \times 11$.

Remarques :

1) L'ensemble $\mathcal{D}^+(0)$ est $\mathbb{N}^*$ et l'ensemble $\mathcal{D}^+(1)$ est $\{1\}$. Tout entier naturel autre que 0 et 1 admet des diviseurs entiers naturels en nombre fini et au moins égal à 2.

2) 0 et 1 ne sont pas des nombres premiers.

3) Deux nombres premiers distincts sont premiers entre eux (car 1 est le diviseur commun).

Exercice n 1

1) Dire pour chacun des entiers s'il est premier ou composé : 4325463213, 56789101244, 235525752.

2) Soit n un entier naturel.

a) Factoriser $5n^2 - 9n$.

b) Pour quelle(s) valeur(s) de n, l'entier $5n^2 - 9n$ est-il premier ?

3) Soit p un entier naturel non nul

a) Montrer que l?un des entiers p, $p+2$, $p+4$ est divisible par 3.

b) En déduire qu'il existe un unique triplet d'entiers naturels $(p, p+2, p+4)$ tel que p, $p+2$, $p+4$ soient premiers.

Réponse

Théorème

- Tout entier naturel différent de 1 admet au moins un diviseur premier.
- Si n est un entier naturel distinct de 1, alors le plus petit diviseur de n distinct de 1 est premier.
- Un entier naturel $n > 1$ est composé, si et seulement si, il admet un diviseur premier inférieur ou égal à $\sqrt{n}$

Démonstration :

- L'ensemble des diviseurs de n, strictement plus grands que n, est non vide car il contient n. Notons p le plus petit élément de cet ensemble. Soit q un diviseur de p. C'est alors un diviseur de n et ce diviseur est inférieur ou égal à p. Ce ne peut donc être que 1 ou p puisque p est le plus petit diviseur de n autre que 1. L'entier p est donc premier.
- Soit p le plus petit élément de $\mathcal{D}^+(n) \setminus \{1\}$. Nous venons de voir que p est premier. Soit a le quotient de n par p : $n = pa$. n n'étant pas premier, a est différent de 1 et c'est aussi un diviseur de n. De ce fait, il est au moins égal à p . Avec $p \leq a$, il vient $p^2 \leq ap$, c'est-à-dire $p^2 \leq n$.Donc $p \leq \sqrt{n}$

En pratique c'est la contra-posée de cette dernière implication qui est utilisée :

« si n n'a aucun diviseur premier, p, tel que : $p \leqslant \sqrt{n}$; alors n est premier ».

Exemple

163 est-il un nombre premier ?
On a : $\sqrt{163} = 12{,}7\cdots$; les nombres premiers p vérifiant : $p \leqslant \sqrt{163}$; sont : 2;3;5;7 et 11. On a : $163 = 2 \times 81 + 1$ et $0 < 1 < 2$: donc 163 n'est pas multiple de 2. $163 = 3 \times 54 + 1$ et $0 < 1 < 3$: donc 163 n'est pas multiple de 3. $163 = 5 \times 32 + 3$ et $0 < 3 < 5$: donc 163 n'est pas multiple de 5. $163 = 7 \times 23 + 2$ et $0 < 2 < 7$: donc 163 n'est pas multiple de 7. $163 = 11 \times 14 + 9$ et $0 < 9 < 11$: donc 163 n'est pas multiple de 11. 163 n'est divisible par aucun des nombres premiers p vérifiant : $p \leqslant \sqrt{163}$; donc 163 est un nombre premier.

Exercice n 2

1) Montrer que 1907 et 1997 sont premiers.

2) a) Montrer que si p est premier et impair, alors il est de la forme $4m+1$ ou $4m+3$, $m \in \mathbb{N}$.

b) Peut-on affirmer que tout entier naturel de la forme $4m+1$ ou $4m+3$ est premier ?

Réponse

Crible d'Eratosthène

Le crible d'Ératosthène est une méthode ancienne et efficace pour trouver tous les nombres premiers inférieurs ou égaux à un entier naturel n. Inventée par **le mathématicien grec Ératosthène** au IIIe siècle avant J.-C., elle repose sur l'élimination progressive des multiples des nombres premiers.

Exemple pour $n = 100$

1) Écrire les nombres de 2 à 100.

2) Prendre le premier nombre non barré (2), barrer ses multiples : $4, 6, 8, \ldots, 100$.

3) Passer au suivant non barré (3), barrer ses multiples : $6, 9, 12, \ldots, 99$.

4) Continuer avec 5 (multiples : $10, 15, 20, \ldots, 100$), puis 7 (multiples : $14, 21, 28, \ldots, 98$).

5) S'arrêter après 7, car $\sqrt{100} = 10$, et tous les nombres premiers inférieurs à 10 ont été traités.

6) Les nombres non barrés sont les nombres premiers.

Après avoir barré tous les multiples, les nombres restants sont les nombres premiers jusqu'à 100 :

2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11
~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~
~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31
~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41
~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~
~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~	61
~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~	71
~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~
~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~
~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~	

Les nombres premiers jusqu'à 100 sont : $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$.

Exercice n 3

Soit q un nombre premier et deux entiers a et b tels que $a = 2q + 1$ et $b = 2 + q$.

1) On suppose que q appartient à l'ensemble $\{3, 5, 7, 11, 13, 17, 19, 23\}$.

- **a)** Pour chaque valeur de q, déterminer les diviseurs premiers de a.
- **b)** Pour chaque valeur de q, déterminer les diviseurs premiers de b.

2) Soit p et q deux nombres premiers distincts.

- **a)** Montrer que l'entier naturel $b = p + q$ admet un diviseur premier distinct de p et de q.
- **b)** Utiliser un raisonnement par l'absurde pour montrer que l'entier naturel $a = pq + 1$ admet un diviseur premier distinct de p et de q.

Réponse .....

Théorème d'Euclide

Il existe une infinité de nombres premiers.

Démonstration :

Soit n un entier naturel non nul, formons l'entier $A = n! + 1$. Soit k un entier appartenant à $\{1, \ldots, n\}$. Puisque $n!$ est un multiple de k, le nombre $A = n! + 1$ n'est pas un multiple de k. Comme A admet au moins un diviseur premier , ce diviseur premier est plus grand que k. En particulier, si n est un nombre premier, il existe un nombre premier plus grand que n. Ceci montre que l'ensemble des nombres premiers n'admet pas de plus grand élément et qu'il est donc infini.

Exercice n 4

1) Vérifier que le $3^{\text{ème}}$ nombre premier est inférieur à $2 \times 3 + 1$.

2) Vérifier que le $4^{\text{ème}}$ nombre premier est inférieur à $2 \times 3 \times 5 + 1$.

3) Soit n un entier naturel non nul, on désigne par p_n le $n^{\text{ème}}$ nombre premier. Montrer que $p_n \leq p_1 \times p_2 \times \ldots \times p_{n-1} + 1$.

Réponse .....

.....

.....

.....

Le théorème fondamental de l'arithmétique

Exercice n 5

Décomposer chacun des entiers ci-dessous en produit de facteurs premiers : 5625, 4160, 14641.

Réponse .....

.....

.....

.....

Théorème

Tout entier naturel n supérieur ou égal à 2 se décompose en un produit fini de nombres premiers.

Démonstration :

- pour $n = 2$ est premier **(vraie)**. Soit n un entier, au moins égal à 2. Supposons que tout entier inférieur ou égal à n est premier ou bien s'écrit d'une manière unique comme produit de facteurs premiers.
- Considérons alors l'entier $n+1$. Soit p le plus petit diviseur premier de $n+1$ et q le quotient de $n+1$ par p. Si $n+1$ n'est pas premier , p n'est pas égal à $n+1$ et il est donc strictement compris entre 1 et $n+1$. Par suite, q est compris entre 2 et n . L'hypothèse de récurrence nous donne que q est premier ou produit de facteurs premiers. Il s'ensuit que $n+1 = pq$ est produit de facteurs premiers.
- **En conclusion,** tout entier $n \geq 2$ est premier ou bien s'écrit comme produit de facteurs premiers d'une manière unique.

Théorème (admis)

Pour tout entier naturel $n \geq 2$, il existe des nombres premiers distincts deux à deux $p_1, \ldots, p_k$ et des entiers naturels non nuls $a_1, \ldots, a_k$ tels que $p_1 < p_2 < \ldots < p_k$ et n se décompose de façon unique sous la forme $\boxed{n = p_1^{a_1} \times p_2^{a_2} \times \ldots \times p_k^{a_k} = \prod_{i=1}^{k} p_i^{\alpha_i}}$.

Exemple

- Décomposer 17640 et 411600 en produits de facteurs premiers.
- En déduire le PGCD et le PPCM de ces deux nombres.

- $17640 = 2 \times 8820 = 2^2 \times 4410 = 2^3 \times 2205 = 2^3 \times 3 \times 735 = 2^3 \times 3^2 \times 245 = 2^3 \times 3^2 \times 5 \times 49$

$$= 2^3 \times 3^2 \times 5 \times 7^2$$

- $411600 = 2 \times 205800 = 2^2 \times 102900 = 2^3 \times 51450 = 2^4 \times 25725 = 2^4 \times 3 \times 8575 = 2^4 \times 3 \times 5 \times 1715$

$$= 2^4 \times 3 \times 5^2 \times 343 = 2^4 \times 3 \times 5^2 \times 7 \times 49 = 2^4 \times 3 \times 5^2 \times 7^3$$

- Le PGCD de 17640 et 411600 est donc $\boxed{2^3 \times 3 \times 5 \times 7^2 = 5880}$
- Le PPCM de 17640 et 411600 est donc $\boxed{2^4 \times 3^2 \times 5^2 \times 7^3 = 1234800}$

Remarque :

Soit a et b deux entiers naturels supérieurs à 1. En mettant en commun leurs diviseurs premiers, on peut écrire : $a = \prod_{i=1}^{n} p_i^{\alpha_i}$ et $b = \prod_{i=1}^{n} p_i^{\beta_i}$.

On a alors : $\boxed{\text{PGCD}(a,b) = \prod_{i=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}}}$; $\boxed{\text{PPCM}(a,b) = \prod_{i=1}^{n} p_i^{\max\{\alpha_i,\beta_i\}}}$

Pour tous entiers naturels α et β, on a : $\min\{\alpha,\beta\} + \max\{\alpha,\beta\} = \alpha + \beta$; on en déduit que :

$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = \prod_{i=1}^{n} p_i^{\min\{\alpha_i,\beta_i\}+\max\{\alpha_i,\beta_i\}} = \prod_{i=1}^{n} p_i^{\alpha_i+\beta_i} = \prod_{i=1}^{n} p_i^{\alpha_i} \cdot \prod_{i=1}^{n} p_i^{\beta_i} = ab.$$

Exemple Pour $a = 550 = 2^1 \times 3^0 \times 5^2 \times 11^1$ et $b = 405 = 2^0 \times 3^4 \times 5^1 \times 11^0$, il vient :

$$\text{PGCD}(550;405) = 2^0 \times 3^0 \times 5^1 \times 11^0 = 5 \quad \text{et} \quad \text{PPCM}(550;405) = 2^1 \times 3^4 \times 5^2 \times 11^1 = 44550$$

Exercice n 6

1) Décomposer en facteurs premiers chacun des nombres $a = 120$ et $b = 75$.

2) En déduire une décomposition en facteurs premiers de : ab, a^2, b^8, $a^2 \vee b^8$ et $a^2 \wedge b^8$.

Réponse .....

.....

.....

.....

.....

Exercice n 7

Un entier naturel est un carré parfait lorsque sa racine carrée est un entier naturel.

1) a) Donner la décomposition en facteurs premiers de chacun des entiers 9801, 57600, 105625.

b) En déduire que chacun de ces entiers est un carré parfait.

2) a) Montrer que l'entier 151875 n'est pas un carré parfait.

b) Quel est le plus petit entier naturel par lequel il faut multiplier 151875 pour obtenir un carré parfait ?

Réponse .....

.....

.....

.....

.....

.....

.....

Exercice n 8

1) a) Montrer que 2311 est un nombre premier.

b) Donner tous les diviseurs de 2311^{2025}. Calculer la somme de tous ces diviseurs.

2) a) Montrer que 5113 est un nombre premier.

b) Donner tous les diviseurs de 5113^{2024}. Calculer la somme de tous ces diviseurs.

3) a) Dénombrer tous les diviseurs de $2311^{2025} \times 5113^{2024}$.

b) Calculer la somme de tous ces diviseurs.

Réponse .....

.....

.....

.....

.....

.....

.....

Théorème

Soit a et b deux entiers naturels et p un nombre premier qui divise le produit ab.

Si p ne divise pas a, alors p divise b.

Démonstration :

- p est un nombre premier, a et b sont des entiers naturels, p divise ab , et p ne divise pas a .
- Puisque p est un nombre premier et p ne divise pas a, les seuls diviseurs positifs de p sont 1 et p. Par conséquent, : $\text{PGCD}(a,p) = 1$.
- Le lemme de Gauss : p est un nombre premier, p divise ab, et $\text{PGCD}(a,p) = 1$, alors p divise b.

Exercice n 9

1) Déterminer tous les entiers naturels a et b tels que $3a = 2b$.

2) Déterminer tous les entiers naturels a et b tels que $5a = 33b$.

3) Déterminer tous les entiers naturels a et b tels que $11(a-2) = 10(b-3)$.

Réponse .....

Exercice n 10

1) Vérifier que 5 divise C_5^k, pour tout $k = 1,2,3,4$.

2) Vérifier que 7 divise C_7^k, pour tout $k = 1,2,3,4,5,6$.

3) Soit p un nombre premier.

a) Vérifier que $kC_p^k = pC_{p-1}^{k-1}$, pour tout $k = 2,3,\ldots,p-1$.

b. En déduire que p divise C_p^k, pour tout $k = 1,2,\ldots,p-1$.

Réponse .....

Exercice n 11

1) Montrer que si p est un nombre premier, alors pour tous entiers naturels a et b, $(a+b)^p - (a^p + b^p)$ est divisible par p.

2) En déduire par récurrence sur a, que pour tout entier naturel a et tout nombre premier p, p divise $a^p - a$.

3) Montrer que pour tout nombre premier p et tout entier naturel a non divisible par p, p divise $a^{p-1} - 1$.

Réponse .....

Petit théorème de Fermat

Soit p un nombre premier et a un entier naturel. Alors p divise $a^p - a$.

Exercice n 12

Soit un nombre premier p et deux entiers naturels a et b.

1) Montrer que si p divise b^2, alors p divise b.

2) Montrer que si p est un diviseur commun de a et de b^2, alors p divise $a \wedge b$.

3) En déduire que si a et b sont premiers entre eux, alors a et b^2 sont premiers entre eux.

Réponse .....

Exercice n 13

Soit le polynôme $f(x) = 8x^3 - 16x - 3$.

1) **a)** Montrer que si n est un entier naturel tel que $f(n) = 0$, alors n divise 3.

b) En déduire que le polynôme f n ?admet pas de racine entière.

2) On se propose de chercher si f admet une racine rationnelle positive. Soit deux entiers naturels a et b premiers entre eux, vérifiant $f\left(\frac{a}{b}\right) = 0$.

a) Montrer que $8a^3 - 16ab^2 - 3b^3 = 0$.

b) En déduire que a divise 3 et que b divise 8.

c) Conclure.

Réponse .....

Exercices à la maison

Exercice n : QCM page 150 ; Exercice n : 2 ;3 ;4 ;5 ;6 ;8 ;9 ;10 page 152 ; Exercice n 11 ; 12 ;13 ;14 page 153